



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,434	11/28/2003	David Lawler Christiansen	MS1-1703US	1238
22801 7590 06/19/2009 LEE & HAYES, PLLC 601 W. RIVERSIDE AVENUE SUITE 1400 SPOKANE, WA 99201				
EXAMINER ARAQUE JR, GERARDO				
ART UNIT		PAPER NUMBER		
3689				
MAIL DATE		DELIVERY MODE		
06/19/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/724,434

Applicant(s)

CHRISTIANSEN, DAVID LAWLER

Examiner

Gerardo Araque Jr.

Art Unit

3689

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 and 13-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11 and 13-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-8508)
Paper No(s)/Mail Date 3/10/09
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Specification

1. The specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. **Claims 1 – 11 and 28** are rejected under 35 U.S.C. 101. Based on Supreme Court precedent and recent Federal Circuit decisions, the Office's guidance to an examiner is that a § 101 process must (1) be tied to a particular machine or apparatus or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876).

To qualify as a § 101 statutory process, the claim should recite the particular machine or apparatus to which it is tied, for example by identifying the machine or apparatus that accomplishes the method steps, or positively reciting the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

There are two corollaries to the machine-or-transformation test. First, a mere field-of-use limitation is generally insufficient to render an otherwise ineligible method

claim patent-eligible. This means the machine or transformation must impose meaningful limits on the method claim's scope to pass the test. Second, insignificant extra-solution activity will not transform an unpatentable principle into a patentable process. This means reciting a specific machine or a particular transformation of a specific article in an insignificant step, such as data gathering or outputting, is not sufficient to pass the test.

Here, applicant's method steps fail the first prong of the new test because the amended limitations where the applicant has stated that the claimed invention is being performed at a computing device is nothing more than an insignificant extra solution activity. Specifically, the Examiner asserts that the applicant has not claimed a particular machine that has been specifically configured to carry out the claimed invention. Although, the method is being performed at a computing device it is asserted that the computing device is not carrying out the claimed invention, but the user of the computing device.

Further, applicant's method steps fail the second prong of the test because it is asserted that the claimed invention is nothing more than the gathering and storing of data. The claimed steps have not transformed anything into another state or thing. Merely gathering data and evaluating the gather data is not considered to be a transformation.

4. **Claims 13 – 27** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Computer-readable medium as described in the specification is defined as being communication connection that comprises of a

wireless signal and at this time, signals are currently considered forms of energy and therefore are non-statutory.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claims 1 – 28** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. In regards to **claim 1**, the Examiner is uncertain as to who is performing the interception of the message. Moreover, because it is unclear on who is performing the interception process it is also unclear on how the intercepting is being performed. Is the intercepting of the message an intermediary step that occurs before the message arrives at its destination by a user. Is it being performed by a computer? Is it a program? Is it a combination of a user, computer, and/or program?

Further still, it is unclear on what the invention is attempting to accomplish. Specifically, the invention discloses an owner of an object and then evaluates whether the owner exceeds a [first] threshold security level. However, it is unclear why an evaluation is ever carried out since it is confusing as to why the owner would be considered to be questionable or dangerous (**Claims 2 and 3**). In other words, because the owner is the creator of the object then it is unclear as to why the owner would be considered to not be trusted.

Moreover, if the entity has access to the object why would an evaluation of a second security threshold level be carried out? In other words, if the entity has access to the object then it is understood that the entity is considered to be trusted.

Consequently, the Examiner then questions on what is the difference between the owner and entity since they are being treated as entities that are not supposed to have access to the object when it has already been determined that they are supposed to have access to the object.

Finally, the Examiner asserts that the claim is incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: what actions are to be carried out if the entity and owner do not exceed the threshold security level.

Similar situations arise in **claims 13 and 19**.

8. **Claim 1** recites the limitation "**the threshold security level**" in **line 10 of claim**

1. There is insufficient antecedent basis for this limitation in the claim. It is asserted that the phrase should read as, "**the first threshold security level**."

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. **Claims 1 – 11 and 13 – 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chan et al. (US PGPub 2002/0019941 A1)**.

11. In regards to **claims 1**, **Chan** discloses a computer-executable method, comprising:

via operations of a processor of a computing device,

intercepting a message at the computing device that modifies security information associated with an object, the security information identifying an owner of the object and an entity that has access to the object (**Page 3 ¶ 36 – 37; Page 6 – 7 ¶ 68 wherein a message that is requesting access (modifying security information) to an object is intercepted and wherein the process of requesting access identifies the owner of the object and the entity that has or is requesting access to the object through the use of tokens, SID, and ACL**);

determining, at the computing device, if the owner exceeds a first threshold security level (**see at least Page 3 ¶ 35 – 37 wherein an SID (security identifier that identifies the owner of the object) is used to determine access rights (security threshold) of the object**); and

determining, at the computing device, if the entity that has access to the object exceeds a second threshold security level (**see at least Page 3 ¶ 35 – 37 wherein, at least, and ACL is used to determine access rights (security threshold) to an object**).

Chan discloses a system and method wherein security rights are determined by identifying the level of access that an object permits, as well as identifying the level of access that an entity has towards the object.

However, **Chan** fails to explicitly disclose:

issuing a first notification that the owner exceeds the [first] threshold security level; and

issuing a second notification that the entity exceeds the second threshold security level.

Despite of this, **Chan** does disclose that failed attempts of accessing an object are logged. In other words, **Chan** discloses that when a user is determined to not have specific access rights to an object the operation is logged. As a result, although **Chan** does not disclose having a first and second notification one having ordinary skill in the art would have recognized that **Chan** provides a system and method wherein a failed operation is logged if a determination is made that an operation exceeds specified access rights (security threshold). As a result, one having ordinary skill in the art of computer science would not have found it uniquely challenging or difficult to create a log whenever a failed operation occurs.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention to create multiple notifications (logs) for each failed operation (exceeding security threshold) in order to keep track of who or what is attempting to modify an object. One having ordinary skill in the art would have found that providing a notification whenever an identified failed computer process to be predictable since it is common business practice to keep track of unauthorized access and determine if security needs to be increased, as well as providing a means of identifying the user or program that is attempting to gain unauthorized access to an object.

12. In regards to **claim 2, Chan** discloses wherein the first threshold security level identifies the owner as being a questionable security risk (**Page 8 ¶ 84 wherein an access evaluation is performed in order to determine whether access can potentially divulge confidential information**).

Furthermore, the name used for describing the threshold value is considered by the Examiner to be non-functional descriptive material. Since the name does not change or alter the steps of the method (or structure of the system) in anyway it is merely describing the event taking place. That is to say, it would not change the steps of the method if the user was titled questionable or dangerous or not trusted etc this title is just used to assist the human mind in understanding the process which would not change regardless of title. If the threshold is exceeded then the user is flagged, if not then there is no flag set these steps are the same regardless of what the flag is called.

13. In regards to **claim 3, Chan** discloses wherein the first threshold security level identifies the owner as being a dangerous security risk (**Page 8 ¶ 84 wherein an access evaluation is performed in order to determine whether access can potentially divulge confidential information**).

Furthermore, the name used for describing the threshold value is considered by the Examiner to be non-functional descriptive material. Since the name does not change or alter the steps of the method (or structure of the system) in anyway it is merely describing the event taking place. That is to say, it would not change the steps of the method if the user was titled questionable or dangerous or not trusted etc this title is just used to assist the human mind in understanding the process which would not

change regardless of title. If the threshold is exceeded then the user is flagged, if not then there is no flag set these steps are the same regardless of what the flag is called.

14. In regards to **claim 4, Chan** discloses wherein not exceeding the first threshold security level identifies the owner as being trusted **(obviously included in that determining that the owner does has access rights identifies the owner as being trusted).**

15. In regards to **claim 5, Chan** discloses further comprising determining if a grant of permissions to the entity exceeds a third security threshold, and if so, issuing a third notification that the grant of permissions exceeds the third security threshold **(Page 4 ¶ 42; Page 9 – 10 ¶ 95; Page 10 ¶ 96 wherein multiple checks can be performed to determine if the entity is properly authorized for specific access rights).**

16. In regards to **claim 6, Chan** discloses wherein the grant of permissions comprises information that describes what access to the object for which the entity is authorized **(Page 5 ¶ 51 wherein specific processes are granted different access rights and wherein each entity has assigned access rights and restrictions; see also Page 10 ¶ 101).**

17. In regards to **claim 7, Chan** discloses wherein the security information is embodied in a security descriptor associated with the object **(see at least Page 3 ¶ 36 wherein a security descriptor embodying security information is associated with an object).**

18. In regards to **claim 8, Chan** discloses wherein the security descriptor further comprises an owner field having a security identifier that identifies a security context

associated with the owner **(see at least Page 3 ¶ 36 wherein the security descriptor further comprises an SID).**

19. In regards to **claim 9, Chan** discloses wherein the security descriptor further comprises a Discretionary Access Control List containing the information about the entity that has access to the object **(see at least Page 3 ¶ 36 wherein the security descriptor further comprises an ACL (wherein the Examiner asserts that the disclosed ACL is equivalent to the claimed DACL)).**

20. In regards to **claim 10, Chan** discloses wherein the information about the entity comprises a security identifier that identifies a security context of the entity, and an access mask that defines permissions granted to the entity **(see at least Page 3 ¶ 36 wherein “Each entry comprises a type (deny or allow) indicator, flags, a security identifier (SID) and access rights in the form of a bitmask wherein each bit corresponds to a permission).**

21. In regards to **claim 11, Chan** discloses wherein intercepting the message comprises hooking an Application Programming Interface (API) that enables the modification to the security information **(see at least Page 4 ¶ 49 wherein an API is provided to interface applications and users with SIDs, such as to accomplish a GUID to SID conversion, represent the SID in human readable form, and so on. See also ¶ 55, 56, 57, 90).**

22. In regards to **claims 13 – 16 and 18 – 24, Chan** discloses a computer-readable medium having computer-executable instructions embodied thereon, the computer-

executable instructions when executed on one or more processors configuring the one or more processors to perform acts comprising:

evaluating a security threat posed by an application modifying an object, via operations comprising:

intercepting a modified security descriptor for an object, the security descriptor including an owner SID field and a DACL, the owner SID field identifying an owner of the object, the DACL identifying at least one entity that has access to the object and access permissions for the entity (**Page 3 ¶ 36 – 37; Page 6 – 7 ¶ 68 wherein a message that is requesting access (modifying security information) to an object is intercepted and wherein the process of requesting access identifies the owner of the object and the entity that has or is requesting access to the object through the use of tokens, SID, and ACL)**

evaluating the owner of the object to determine if the owner is categorized as dangerous, and if so, issuing an alert notification (**see at least Page 3 ¶ 35 – 37 wherein an SID (security identifier that identifies the owner of the object) is used to determine access rights (security threshold) of the object; Page 8 ¶ 84 wherein an access evaluation is performed in order to determine whether access can potentially divulge confidential information)**;

evaluating the DACL to determine if the entity is categorized as dangerous, and if so, issuing the alert notification (**see at least Page 3 ¶ 35 – 37 wherein, at least, and ACL is used to determine access rights (security**

threshold) to an object; Page 8 ¶ 84 wherein an access evaluation is performed in order to determine whether access can potentially divulge confidential information); and

if the entity is not categorized as trusted, evaluating the DACL to determine if the access permissions for the entity are categorized as dangerous, and if so, issuing the alert notification (see at least Page 3 ¶ 35 – 37 wherein, at least, and ACL is used to determine access rights (security threshold) to an object; Page 8 ¶ 84 wherein an access evaluation is performed in order to determine whether access can potentially divulge confidential information).

Chan discloses a system and method wherein security rights are determined by identifying the level of access that an object permits, as well as identifying the level of access that an entity has towards the object.

However, Chan fails to explicitly disclose:

issuing a first notification that the owner exceeds the [first] threshold security level; and

issuing a second notification that the entity exceeds the second threshold security level.

Despite of this, Chan does disclose that failed attempts of accessing an object are logged. In other words, Chan discloses that when a user is determined to not have specific access rights to an object the operation is logged (Page 3 ¶ 38). As a result, although Chan does not disclose having a first and second notification one having ordinary skill in the art would have recognized that Chan provides a system and method

wherein a failed operation is logged if a determination is made that an operation exceeds specified access rights (security threshold). As a result, one having ordinary skill in the art of computer science would not have found it uniquely challenging or difficult to create a log whenever a failed operation occurs.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention to create multiple notifications (logs) for each failed operation (exceeding security threshold) in order to keep track of who or what is attempting to modify an object. One having ordinary skill in the art would have found that providing a notification whenever an identified failed computer process to be predictable since it is common business practice to keep track of unauthorized access and determine if security needs to be increased, as well as providing a means of identifying the user or program that is attempting to gain unauthorized access to an object.\

In regards to **claims 21, 22, and 24** wherein a second notification is issued if the entity/owner is categorized as dangerous, **Chan** discloses multiple checks can be performed to determine if the entity is properly authorized for specific access rights **(Page 4 ¶ 42; Page 9 – 10 ¶ 95; Page 10 ¶ 96 wherein multiple checks can be performed to determine if the entity is properly authorized for specific access rights)**. With that said, it is asserted that one having ordinary skill in the art looking upon **Chan** and the explanation above regarding the issuing of notifications that it would have been obvious to provide multiple notifications for each event that has occurred. In other words, **Chan** discloses that operations are logged and, as a result, it would have

been obvious that whenever a determination is made on the discussed operation (failed event) the operation(failed event) would be logged.

23. In regards to **claim 17**, Chan discloses wherein the notification comprises an immediate notice issued to a user (**Page 3 ¶ 38; as discussed above, when an issue arises the operation is logged. One having ordinary skill in the art would have not found it uniquely challenging or difficult to log the even after it has occurred. Moreover, the time in which the event is logged is irrelevant and merely a design choice since the time in which the event is logged provides no additional functionality to the steps of the claim. As claimed, one having ordinary skill in the art would have recognized that the amount of elapsed time in which an event is logged does not affect the steps of determining questionable access to an object.**).

24. In regards to **claim 25**, Chan discloses wherein the security information is contained in a security descriptor associated with the object (**Page 3 ¶ 36; Page 6 – 7 ¶ 68 wherein an SID is used which contains security information associated with the object**).

25. In regards to **claim 26**, Chan discloses wherein the security identifier is contained within a DACL (**Page 3 ¶ 36; Page 6 – 7 ¶ 68 wherein an ACL is used which contains the SID**).

26. In regards to **claim 27**, Chan discloses wherein the access rights are described in the DACL (**Page 3 ¶ 36; Page 6 – 7 ¶ 68 wherein an ACL is used which contains access rights**).

27. In regards to **claim 28**, **Chan** discloses wherein:

interception of the message launches an application in a controlled execution environment (Page 3 ¶ 36 – 37; Page 6 – 7 ¶ 68 wherein a message that is **requesting access (modifying security information) to an object is intercepted; see also see at least Page 4 ¶ 49 wherein an API is provided to interface applications and users with SIDs, such as to accomplish a GUID to SID conversion, represent the SID in human readable form, and so on. See also ¶ 55, 56, 57, 90);**

the owner is categorized into one of a plurality of risk categories (Page 5 ¶ 51 **wherein allowed process may be granted different access rights);**

the entity is categorized into one of a plurality of trust types such that in an event the entity is not a trusted entity, the plurality of trust types comprise unknown, public, questionable, and dangerous (Page 5 ¶ 51; Page 8 ¶ 84 **wherein allowed process may be granted different access rights and wherein the entity is evaluated to determine whether they pose a threat to confidential information);**

the method further comprising:

determining, at the computing device, a level of access permissions granted in an access control entry (ACE) (Page 5 ¶ 51 **wherein allowed process may be granted different access rights; see also Page 3 ¶ 36 wherein the contents of the security descriptor are typically determined by the owner of the object and generally comprise a (discretionary) access**

control list (ACL) of access control entries, and for each entry, one or more access rights (allowed or denied actions) corresponding to that entry); and

based at least in part on a level of risk of the level of access permission granted in the ACE, issuing a third notification in an event the access permissions exceed a third threshold security level (**Page 4 ¶ 42; Page 9 – 10 ¶ 95; Page 10 ¶ 96 wherein multiple checks can be performed to determine if the entity is properly authorized for specific access rights**).

Response to Arguments

28. Applicant's arguments with respect to **claims 1 – 28** have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure can be found in the PTO-892 Notice of References Cited.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gerardo Araque Jr. whose telephone number is (571)272-3747. The examiner can normally be reached on Monday - Friday 8:30AM - 4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Janice Mooneyham can be reached on (571) 272-6805. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/G. A./
Examiner, Art Unit 3689
6/17/09

/Dennis Ruhl/
Primary Examiner, Art Unit 3689